

**TROUTMAN PEPPER HAMILTON SANDERS LLP**

Deborah Kovsky-Apap (NJ Bar No. 030942003)

875 Third Avenue

New York, NY 10022

(212) 808-2726

deborah.kovsky@troutman.com

*Counsel for the Ad Hoc Committee of  
Wallet Account Holders*

**UNITED STATES BANKRUPTCY COURT  
DISTRICT OF NEW JERSEY**

In re:

BLOCKFI INC., *et al.*<sup>1</sup>

Debtors.

Chapter 11 Case No. 22-19361 (MBK)

(Jointly Administered)

**HEARING DATE AND TIME:** January 17, 2023, at  
10:00 a.m. (EST)

**STATEMENT OF THE AD HOC COMMITTEE OF WALLET ACCOUNT HOLDERS  
IN SUPPORT OF THE DEBTORS' REDACTION MOTION**

The Ad Hoc Committee of Wallet Account Holders (the "Ad Hoc Committee"), through its undersigned counsel, submits this statement in support of the Debtors' motion to redact client names and other personally identifiable information [Docket No. 4], and respectfully states as follows:

1. The Ad Hoc Committee recognizes the presumption of public access to judicial records, and appreciates the critical importance of transparency in a chapter 11 case. However, as the Debtors correctly point out, that presumption gives way in some circumstances to the need to

---

<sup>1</sup> The Debtors in these Chapter 11 Cases, along with the last four digits of each Debtor's federal tax identification number, are: BlockFi Inc. (0015); BlockFi Trading LLC (2487); BlockFi Lending LLC (5017); BlockFi Wallet LLC (3231); BlockFi Ventures LLC (9937); BlockFi International Ltd. (N/A); BlockFi Investment Products LLC (2422); BlockFi Services, Inc. (5965) and BlockFi Lending II LLC (0154). The location of the Debtors' service address is 201 Montgomery Street, Suite 263, Jersey City, NJ 07302.

protect the financial and physical safety of private individuals. This case presents just such circumstances.

2. The Debtors' disclosure of clients' names, particularly if coupled with account balance information, would effectively paint targets on the backs of hundreds of thousands of individuals. The forced disclosure of that information in the Celsius bankruptcy—even without email addresses—led directly to online harassment and phishing scams. *See, e.g.*, Supplemental Notice of Phishing Attempts, *In re Celsius Network LLC*, Case No. 22-10964-MG (Bankr. S.D.N.Y. Dec. 13, 2022) (describing phishing scams targeting Celsius customers).

3. Even worse: clients' physical safety would be put at risk by public disclosure of the amounts of cryptocurrency that they withdrew from BlockFi, given the assumption that much of that cryptocurrency likely now resides in hardware wallets such as those made by Ledger. As the Official Committee of Unsecured Creditors ("UCC") points out, hackers and thieves are able to cross-reference bankruptcy disclosures with information leaked from unrelated database breaches, including the recent hack of Ledger itself (which exposed physical addresses).<sup>2</sup> In short, forcing the Debtors to disclose clients' names and amounts of withdrawals would be akin handing thieves a roadmap to the precise locations where large amounts of cryptocurrency are being stored on small and highly portable devices. It would make every BlockFi client—whether or not they are actually self-custodying coins—a potential target for home invasion and theft.

4. Section 107(c) is intended to protect individuals from this kind of unwarranted and unnecessary risk. That section allows the Court to limit disclosure of certain types of information that "would create undue risk of identity theft or other unlawful injury to the

---

<sup>2</sup> *See* "Is Ledger Still Safe? Everything We Learned from Last Year's Hack," *CryptoVantage*, available at <https://www.cryptovantage.com/news/is-ledger-still-safe-everything-we-learned-from-last-years-hack/>.

individual or the individual's property," including "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual." See 11 U.S.C. § 107(c)(1); 18 U.S.C. § 1028(d). Commentators have observed that the addition of § 107(c) to the Bankruptcy Code in 2005 "broadened the situations in which the court could protect individuals from disclosure of sensitive information in light of the emerging problem of identity theft and also the possible need to protect individuals from domestic violence or other injury." 2 COLLIER ON BANKRUPTCY ¶ 107.LH[2] (Alan N. Resnick & Henry J. Sommer eds., 16th ed.).

5. In evaluating a redaction request under section 107(c), a court should "balance concerns for impairing . . . judicial efficiency against the privacy interests of the person resisting disclosure." *In re Avaya, Inc.*, No. 17-10089 (SMB), 2019 WL 1750908, at \*5 (Bankr. S.D.N.Y. Mar. 28, 2019). "While a specific potential harm must be identified, the standard does not require evidence of injury having occurred in the past or under similar circumstances." *In re Motions Seeking Access to 2019 Statements*, 585 B.R. 733, 751 (D. Del. 2018), *aff'd sub nom. In re A C & S Inc.*, 775 F. App'x 78 (3d Cir. 2019) (noting that "[s]ection 107(c) references 'risk,' and **assessment of risk is forward-looking**") (emphasis added).

6. Here, the Debtors, the UCC and the Ad Hoc Committee have identified specific potential harms that may result from the broadcasting of the names of clients and their cryptocurrency holdings. The risk to individuals from such disclosure is unacceptably high.

7. Conversely, as noted in the Debtors' Motion, the personally identifiable information for individual clients has been or will be provided to the Court, the United States Trustee ("UST") and the Official Committee of Unsecured Creditors, and may be made available to anyone who needs it for a legitimate, case-related purpose. Under these circumstances, it

seems clear that “judicial efficiency” will be minimally impaired, if at all, by the redaction of clients’ PII—and that any such impairment is significantly outweighed by the potential harm to individuals that could result from the publication of their personal information.

8. The UST’s arguments to the contrary are unavailing. Indeed, in purporting to “balance” the competing interests here, the UST gives virtually no weight to the very real (as demonstrated in the Celsius case) risk of harm to individuals who have been dragged involuntarily into these proceedings. The UST further contends that because clients’ information can be shared with certain third parties pursuant to BlockFi’s Privacy Policy, that information is not protectable under section 107. This argument is disingenuous at best. The UST is surely aware that there is a world of difference between securely sharing information with a discrete set of business partners or government entities, and broadcasting it over the internet.

9. BlockFi’s individual clients have suffered harm enough from BlockFi’s insolvency and bankruptcy filing. They should not be victimized twice by having their personally identifiable information made public to the entire world.

### **CONCLUSION**

For the foregoing reasons, the Ad Hoc Committee requests that the Court grant the Debtors’ Motion with respect to the redaction of individual customers’ names and other personally identifiable information.

Dated: January 15, 2023

s/ Deborah Kovsky-Apap  
Deborah Kovsky-Apap (NJ Bar No. 030942003)  
875 Third Avenue  
New York, New York 10022  
(212) 704-6000  
deborah.kovsky@troutman.com

*Counsel for the Ad Hoc Committee of  
Wallet Account Holders*